Statement of

Benjamin H. Wu

Assistant Secretary for Technology Policy Nominee
U.S. Department of Commerce

Before the

Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations

"Smart Card Activities of the
National Institute of Standards and Technology"

October 6, 2004

Chairman Buyer, Ranking Member Hooley, Members of the Subcommittee, thank you for this opportunity to testify today about the National Institute of Standards and Technology's (NIST) activities related to the advancement of smart card and biometric technologies within the Federal government. You are to be commended for your leadership to implement smart card technology at the Department of Veterans' Affairs. NIST plays an important role in cooperation with other Federal agencies, to eliminate the road blocks to widespread deployment of smart cards. As part of the Department of Commerce's Technology Administration, NIST is working with industry and other government agencies to provide interoperability specifications, standards, and guidelines with the goal of expediting open and interoperable methods for using smart cards. NIST will be leading the President's assignments to the Department of Commerce required by the Homeland Security Presidential Directive/Hspd-12, "Policy for a Common Identification Standard for Federal Employees and Contractors." NIST has also done considerable work in the area of biometrics under the auspices of the USA Patriot Act.

Background

Smart cards provide opportunities for improving security of our critical infrastructure, both from a physical and logical perspective. Because they are capable of performing cryptographic functions, they can perform important security services such as securely storing digital signatures, holding public key credentials, and authenticating a claimed identity based on biometric data. As such, smart cards are a crucial element in a range of current and expected critical applications and programs. They are also the underlying foundation for the standard required by Hspd-12.

NIST's smart card program dates back to 1988. Recognizing the potential for smart cards to improve the security of Federal IT systems and our national information infrastructure, NIST chose to invest significant research effort in smart card technology at an early stage. The NIST smart card program produced many early innovations in the area such as a generic authentication interface for smart cards, the first cards to implement the Data Encryption Algorithm and the Digital Signature Algorithm, and the first reprogrammable smart card. These innovations are integral to modern smart cards.

Many Federal agencies have a longstanding interest in smart card technology. However, large-scale deployment of smart cards has proven challenging. A survey revealed that agencies found it difficult to deploy large-scale smart card systems due to a lack of interoperability among different types of smart cards and without assurances of interoperability, agencies would be "locked" into a single vendor. Thus, the issue of interoperability had to be addressed before significant investments were made. Additionally, smart card systems have historically been driven by requirements arising from specific application domains such as banking, telecommunications, and health care. This has led to the development of smart cards that are customized to the specific application requirements of each domain, with little interoperability between domains. These vertically-structured smart card systems are expensive, difficult to maintain, and

often based on proprietary technology.

GSA created a contract vehicle and program to procure interoperable smart card systems and services and to promote and facilitate the use of this critical security technology within the Federal sector. After much work to address the Federal customer needs identified, NIST published two versions of the Government Smart-Card Interoperability Specification in June 2002 and July 2003, respectively. (Available via http://smartcard.nist.gov/ .)

The GSC-IS has been well received and is making a significant impact. Many Federal agencies are moving forward with plans to deploy large numbers of GSC-compliant systems. The Department of Defense's Defense Manpower Data Center, Common Access Card (CAC) Program Office has stated the following about NIST and smart cards:

> *Our department recognizes the …technical skill and leadership in the area of Smart Card Interoperability and building the Government Smart Card Interoperability Specification… vital to the interests of our Department as well as a major contribution in the Federal Sector regarding national security.*

DoD has adopted the Interoperability Specification for their enterprise-wide CAC deployment, representing millions of cards (to be effective in 2004.)

Standardization

GSA and other Federal agencies have long sought to avoid the problem of being locked into proprietary, non-interoperable smart card technologies. Recognizing the needs of the Federal customer base, NIST is working with American National Standards Institute (ANSI) and the International Organization for Standardization (ISO) to standardize this specification. ANSI carried a new work item to ISO that was based on the NIST smart card work. This new work item was balloted and overwhelmingly approved by the national bodies. Of the 24 countries voting, 19 voted yes, two did not cast a vote, and two votes were qualified no's that later changed to 'yes'. An international task force has been established, with NIST as the chair. The work of this task force is to develop a new suite of smart card interoperability standard, which are based on NIST IR 6887 – Government Smart Card Interoperability Specification. This Task Force was established in April of 2004 and has already met twice, has a new work programme approved, has been given an ISO number for this new suite of standards, (ISO 24727) and is scheduled to provide drafts in March of 2005. The Task Force has the backing of the international community and is moving very aggressively and plans to have approved standards within 24 months, which is very aggressive for an international effort.

Additionally, ANSI has established a new national work group to address national smart card interoperability standards work. This group is chaired by NIST.

In summary, in the last 11 months NIST has successfully accomplished significant steps in the formal standards world by being the leading and driving force in 1) the establishment of a formal ANSI Task Group to address smart card interoperability at a National level, 2) the overwhelming approval for a new international standard and 3) the establishment of an international Task Force, with support to Chair this new group.

The Government Accountability Office (GAO) issued a report in January 2003 on the Federal government's progress in adopting smart card technology. The report stated:

> *We recommend that the Director, NIST, continue to improve and update the government smart card interoperability specification by addressing governmentwide standards for additional technologies – such as contactless, biometrics, and optical stripe media – as well as integration with PKI, to ensure broad interoperability among Federal agency systems.*

In response to these GAO recommendations and identified Federal agency needs, NIST is examining requirements for and issues associated with definition of a multi-technology card platform. Technologies being investigated for utility in a multi-technology platform include smart card integrated circuits, optical stripe media, bar codes, magnetic stripes, photographs, and holograms. As a first step, NIST hosted a workshop on multi technology card issues in July of this year. The workshop focused on requirements, issues, and Federal government activities associated with multi-technology cards. More specifically, it examined general technical and business issues, existing voluntary industry consensus standards, gap areas in standards coverage, and industry capabilities in the field of ISO/IEC 7810-compliant storage and processor card technologies. The workshop also addressed multi technology integration issues, and both inter-jurisdictional and inter-technology interoperability issues.

Based on the proceedings of the workshop and subsequent interviews conducted with the user community, NIST produced a technical report that identified integration and interoperability research topics, gaps in standards coverage, and multi-technology composition issues. This was completed in March 2004.

NIST published the GSC-IS, Version 2.1 in July 2003 as NISTIR 6887, 2003 Edition. This document addresses the remaining GAO recommendations by providing support for biometrics, contactless smart card technology, and Public Key Infrastructure.

There is considerable interest in the convergence of biometrics and smart cards. In response to requirements from the GSC customer base and recommendations in the GAO Report, NIST has included 'hooks' for biometric authentication modules in Version 2.1 of the GSC Interoperability Specification. During FY03, NIST also worked with an ANSI M1 ad hoc group to publish an analysis of existing biometric and smart card interoperability standards with respect to their ability to support integrated smart card-biometric systems. The report includes detailed recommendations for designing a GSC biometric plug-in framework. It has been submitted to ANSI B10 to provide a roadmap for integrating full biometric capabilities into the GSC framework during the formal

standards development process. Published August 2003, the report is available to the general public on the ANSI/INCITS M1 document register (http://www.incits.org/tc_home/m1htm/docs/m1030398.pdf.).

Moreover, NIST is actively working with Europe and Japan towards a general smart card framework that can harmonize and align a variety of disparate approaches, technologies, and architectures. We believe that this would yield greater interoperability, lower costs and barriers, and enhanced security.

Smart Card Conformance Testing

Conformance testing is an important and integral element of a standards program. It can increase the confidence for consumers that a given product does conform to a given specification reducing the risk to the purchaser. NIST has been developing an interoperability conformance test program in parallel with the GSC standards effort. The GSC conformance test program will rely on commercial laboratories to validate conformant products, providing customers with increased assurance that these products meet the interoperability requirements of the GSC framework. NIST conformance test engineers and programmers are developing test criteria and building a suite of conformance test tools to be used by commercial laboratories to test and ultimately improve private-sector smart card products.

Homeland Security Presidential Directive -12

Hspd-12 was issued on August 27th, 2004. The directive calls for the Secretary of Commerce to issue a Federal standard for secure and reliable forms of identification (ID) issued by the Federal Government to its employees and contractors (including contractor employees). This standard will serve as the basis for the creation of a secure and reliable ID that, 1) is issued based on sound criteria for verifying an individual employee's identity, 2) is strongly resistant to identity fraud, counterfeiting, and terrorist exploitation, 3) can be rapidly authenticated electronically and 4) is issued only by providers whose reliability has been established by an official accreditation process. The standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application.

This is obviously quite an ambitious assignment and one that will considerably aid the homeland security efforts of the Federal Government. While developing the standard required by Hspd-12, we will ensure that ample privacy protections are included.

Within the Technology Administration, NIST is taking the lead in developing this standard and has developed an ambitious timetable to meet the six-month deadline. NIST is working with the Office of Management and Budget and other departments and agencies to take advantage of efforts currently underway within the Federal Government.

NIST will also be working with the public and private sectors to develop the standard. Today, NIST is holding a workshop with over 80 Federal agency representatives to discuss the development of this standard. Additionally, tomorrow (October 7, 2004), NIST is holding a public workshop for industry and others to discuss its plans and to solicit ideas and feedback.

Further Research and Development

Smart cards and associated technologies hold great promise for meeting many important needs in homeland security. Success in large-scale deployments of smart cards and their associated applications, however, is not assured. As a community, we will have to be innovative in finding ways to fund and develop the needed tools, tests, examples, frameworks, best practices, and research to deliver scalable, secure, and interoperable smart card infrastructure and associated applications.

Some of these tasks include the development of reference implementations, software developer's toolkits, data models, issuance policies, credential management, publication of implementation guidance, pilot projects and continued research and development. An educational program to share information and avoid duplication of effort would be of great benefit as well. Most of the Federal agencies that comprise the GSC community have budgets for their own smart card deployments, but these budgets do not include support for an interagency research and development program. Developing standards is critical to ubiquitous adoption (and achieving the attendant security benefits) of smart cards, and this work will continue to be of great importance.

Summary

The U.S. GSC-IS has generated considerable interest and support in both the U.S. domestic and international smart card communities. By developing a viable commercial market place for smart card technology in the U.S., we can increase the competitiveness of the U.S. smart card industry in the global market, while improving the security of our nation’s critical infrastructure. NIST is continuing to improve and update smart card interoperability specifications and actively participate in Federal coordinating efforts. The smart card work will also play a key role in developing Federal employee credentials required by Hspd-12.

I would be pleased to answer any questions you may have.